

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
9 January 2003 (09.01.2003)

PCT

(10) International Publication Number
WO 03/003587 A2

(51) International Patent Classification⁷: **H04B**
(21) International Application Number: **PCT/IB02/02469**
(22) International Filing Date: **27 June 2002 (27.06.2002)**
(25) Filing Language: **English**
(26) Publication Language: **English**
(30) Priority Data:
09/893,523 **29 June 2001 (29.06.2001)** **US**
(71) Applicant (for all designated States except US): **NOKIA CORPORATION [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).**

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(72) Inventors; and
(75) Inventors/Applicants (for US only): **NELGER, Rickard [SE/SE]; Landgången 32, S-591 72 Motala (SE). NIEMI-NEN, Ari [FI/SE]; Karolinerväg 9, S-591 97 Motala (SE).**
(74) Agents: **WALASKI, Jan et al.; Venner, Shipley & Co., 20 Little Britain, London, EC1A 7DH (GB).**

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: **CONDITIONAL ACCESS SYSTEM**

(57) Abstract: A conditional access system in which entitlement control messages (ECMs) containing the encryption keys used to encrypt a programme transmission, are sent to a set-top box over a secure communications channel separate from the channel used for transmission of the encrypted programme.

WO 03/003587 A2



Conditional Access System

Field of the Invention

The present invention relates generally to the field of broadcast and reception,
5 particularly but not exclusively to a conditional access system in a digital satellite television system. More particularly, aspects of the present invention relate to the transfer of entitlement control messages in a channel separate from the broadcast channel.

10 Background

Conditional access systems are well known and widely used in conjunction with currently available pay television systems. At present, such systems are based on the transmission of programmes scrambled with control words which are received by subscribers having a set-top box and a smart card for each subscription package.
15 The smart card for a subscription package from a particular service provider allows the scrambled programmes within the package to be descrambled and viewed. The broadcast stream further contains entitlement management messages and entitlement control messages, which are necessary for the smart card to descramble the broadcast. The terms scrambled and encrypted are used interchangeably in this
20 application.

WO 98/43426 discloses a digital satellite television system in which the entitlement management messages are transmissible to the set-top box via a modem based back channel, rather than via the broadcast channel. This is done to speed up viewer
25 authorisation in viewing systems such as pay-per-view, since there is a certain time delay before the subscriber authorisation system (SAS) can include the proper entitlement management messages in the broadcast stream. However, the entitlement control messages which contain the control word in an encrypted format are sent via the broadcast channel. The control word is decrypted at the set-
30 top box by means of a smart card.

Summary of the Invention

According to the present invention, there is provided a conditional access system comprising a first transmitter for transmitting a scrambled broadcast stream and a second transmitter for transmitting a plurality of control messages separate from the broadcast stream, said control messages including information for descrambling the
5 broadcast stream.

The control messages may be sufficient on their own to allow the broadcast stream to be descrambled.

10

By separating the broadcast and control message channels, the need for a smart card can be obviated, since the information for descrambling the broadcast stream can be incorporated in said control messages without being encrypted. While the control messages can then be encrypted for transmission over a secure link, for example
15 over a virtual private network using a protocol such as the https secure sockets protocol, the unencrypted control words are recovered at the receiver side of the secure link, so that the decoder does not require a smart card for decryption. Advantageously, since the decoder is thereby provided with ready to use decryption keys, the decoder can be made to be independent of any specialised conditional
20 access system.

Additional security can be provided by encrypting the information for descrambling the broadcast stream into the control messages, which gives rise to the need for a smart card, such as a virtual or software smart card, at the decoder.

25

According to the invention, there is further provided a conditional access system comprising a first receiver for receiving a scrambled broadcast stream and a second receiver for receiving a plurality of control messages separate from the broadcast stream, the control messages including information for descrambling the broadcast
30 stream.

The invention further provides a decoder for use in a conditional access system for decrypting encrypted broadcast content, comprising a first input module for receiving said encrypted broadcast content from a first communications channel and a second input module for receiving a plurality of control messages from a second communications channel, said control messages containing descrambling information for decrypting said broadcast content.

According to the invention, there is also provided a method for use in a conditional access system, in which a scrambled broadcast stream is transmitted to a decoder, said decoder being operable to receive a plurality of control messages including information for descrambling the broadcast stream, the method comprising sending said control messages to said decoder separately from said broadcast stream.

The invention yet further provides a method for use in a conditional access system, in which a scrambled broadcast stream is transmitted to a first decoder and a second decoder, said first and second decoders being operable to receive a plurality of control messages including information for descrambling the broadcast stream, the method comprising receiving a request to transmit a plurality of control messages to said second decoder separately from the broadcast stream.

Roaming can thereby be facilitated. By denying a service to the first decoder while the control message stream is being sent to the second decoder, use of the service at the subscriber's home location can be prevented whilst roaming.

The first decoder does not need to have the ability to receive control messages separately and can be a conventional decoder.

According to the invention, there is additionally provided a conditional access system, comprising a first communications channel for carrying a broadcast stream, said stream being scrambled with a stream of control words and a second communications channel separate from the first channel for carrying a stream of entitlement control messages, said entitlement control messages incorporating

information relating to the stream of control words for descrambling the broadcast stream.

The entitlement control messages can alone contain all of the information required to descramble the broadcast stream, so that there is no need for other messages, such as entitlement management messages, to be transmitted. Furthermore, in this case, a decoder for descrambling the broadcast stream does not require a smart card.

10 Brief Description of the Drawings

Embodiments of the invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a schematic diagram of a conventional conditional access system;

Figure 2 is a schematic diagram illustrating the flow of encrypted information and control information in the system of Figure 1;

Figure 3 is a schematic diagram illustrating a conditional access system according to the invention;

Figure 4 is a flow diagram illustrating the operation of the system of Figure 3; and

Figure 5 is a schematic diagram illustrating the flow of encrypted information and control information in the system of Figure 3.

Detailed Description

Referring to Figure 1, in a conventional conditional access system, content to be broadcast, including for example, video, audio and data components, is encoded in an encoder 1 using an appropriate coding system, for example MPEG-II for digital broadcasting. The encoded broadcast stream is encrypted or scrambled in a scrambler 2 under the control of a control word CW generated by a control word generator 3 in a manner which is well-known per se. The control word is encrypted into an Entitlement Control Message (ECM) by an ECM generator 4 together with access criteria which identify the service and the conditions required to access the service. For example, the access criteria may specify regional limitations on the broadcast. A further type of message, referred to as an Entitlement Management Message (EMM), which carries details of the subscriber and his subscription is

generated by an EMM generator 5. While an ECM message is associated with a scrambled programme or set of programmes and carries the information required to decrypt those programmes, an EMM message is a message dedicated to an individual user or group of users and carries the information necessary to determine whether those users have the necessary subscriptions in place to be able to view the programmes.

The scrambled encoded broadcast stream together with the ECM and EMM messages is multiplexed in a multiplexer 6 with other broadcast streams representing other programmes, together making up a subscription package from a particular service provider. The package is sent to a transmitter 7 from which it is transmitted, via a communications channel 8, for example a satellite or cable channel, using an appropriate modulation scheme. The scrambled encoded broadcast stream is received at a subscriber's receiver 9, for example a satellite dish, and passed to the subscriber's set-top box 10.

On receipt at a set-top box (STB) 10, the received data is demultiplexed in a demultiplexer 11, to extract the required programme and its associated ECM and EMM messages. The extracted ECM and EMM messages are sent to a plug-in smart card 12. The smart card 12 uses the ECM and EMM messages to determine whether the subscriber has the right to view the broadcast and if so, to decrypt the control word CW, which is input to a descrambler 13 together with the scrambled broadcast stream to recover the original MPEG-II encoded broadcast stream. The encoded stream is passed to an MPEG-II decoder 14 which produces an output signal comprising audio, video and data components for display on the subscriber's television 15.

The control word comprises alternating odd and even control words which are alternated at, for example, two second intervals. Each control word is changed at predetermined intervals, for example, every twenty seconds. A continuous stream of ECM messages is therefore required to descramble the scrambled signal. The EMM message can be updated less frequently.

The conventional form of ECM and EMM messages is defined in the international standard ISO IEC 13818-1, the entire contents of which are incorporated herein by reference.

5 Figure 2 illustrates the flow of signal data and the control word (CW) within the system of Figure 1. On the transmitter side, the control word CW is used to encrypt the unencrypted broadcast signal S in the scrambler 2 to generate an encrypted signal E(S). This is passed to the multiplexer 6 together with the encrypted control word E(CW) generated by the encryption module 4. On the
10 receiver side, the encrypted signal E(S) and encrypted control word E(CW) from the multiplexer 6 are fed to the demultiplexer 11. This outputs the encrypted signal E(S) to the descrambler 13 and the encrypted control word E(CW) to the smart card decryption module 12. The smart card 12 contains the cryptographic key necessary to decrypt the encrypted control word E(CW) to reproduce the original control
15 word CW. This is used in the descrambler 13 to descramble the encrypted signal E(S) to reproduce the original signal S.

Figure 3 shows an embodiment of the invention which is a modification of the system of Figure 1. In the conditional access system shown in Figure 3, rather than
20 sending the ECM messages along with the broadcast channel, the ECM messages are sent on a separate channel. Referring to Figures 3 and 4, broadcast content is encoded using an MPEG-II encoder 1 (step s1). A control word is generated by a control word generator 3 (step s2) and the encoded broadcast stream is encrypted or scrambled in a scrambler 2 under the control of the control word CW (step s3). The
25 scrambled programme is multiplexed with a plurality of other programmes (step s4) in a multiplexer 6 and transmitted from a transmitter 7 via communications channel 8 to a receiver 9, together comprising, for example, a satellite communications link (step s5). A demultiplexer 11 extracts the required programme stream from the received signal (step s6), which is then sent to a set-top box 20, also referred to
30 herein as a decoder (step s7). The decoder includes a descrambler 13 for descrambling the scrambled broadcast signal under the control of a control word.

An ECM server 21 is used to generate an ECM message which incorporates the control word CW without encryption (step s8), together with the access criteria described with reference to Figure 1. The subscription information which would conventionally be carried by an EMM message is incorporated into the ECM message. The ECM message is not multiplexed into the broadcast stream, but is sent to a second transmitter 22, from where it is transmitted by a second communications channel 23 to a second receiver 24 (step s9). The ECM message is passed from the second receiver 24 to a processor 25 within the set-top box 20 (step s10). The processor 25 checks that the subscription information in the ECM is valid and extracts the control word CW from the ECM message (step s11). This is input to the descrambler 13 (step s12). The descrambler 13 descrambles the broadcast stream using the control word (step s13). The descrambled encoded stream is passed to an MPEG-II decoder 14 which produces an output signal comprising audio, video and data components (step s14) which is sent for display on the subscriber's television 15 (step s15).

The communications channel 23 in this embodiment comprises a virtual private network (VPN). In other embodiments of the invention, the communications channel 23 comprises a cellular telephone network such as a GSM, UMTS or GPRS network, a conventional PSTN point-to-point telephone connection, a DSL connection, a secure HTTPS socket connection over the Internet, another IP based network, for example using streaming media, or a network based on a different protocol or any other form of communications link over satellite, cable, by terrestrial transmission or otherwise. In preferred embodiments of the invention, a secure link is used to enhance the security of the transmitted control word.

In the event that the receiver 24 comprises a mobile telephone, this can be linked to the set-top box by any suitable means, including for example, a cable or infra-red connection.

While Figure 3 shows the second receiver 24 as separate from the set-top box 20, in an alternative embodiment, the second receiver 24 is located within the set-top box 20, as shown by the dotted line marked 26 in Figure 3. For example, the second

receiver 24 provides a network connection which permits the set-top box 20 to be plugged into an appropriate network to provide the ECM message stream.

Figure 5 illustrates the flow of signal data and the control word (CW) within the system of Figure 3. On the transmitter side, the control word CW is used to encrypt the unencrypted broadcast signal S in the scrambler 2 to generate an encrypted signal E(S). The encrypted signal E(S) is sent to the descrambler 13 on the receiver side, via the multiplexer 6 and demultiplexer 11. The control word CW is sent unencrypted to the transmitter 22 where it is encrypted for transmission over a virtual private network 23. The control word CW is decrypted at the receiver 24 and sent to the descrambler 13 in unencrypted form, where it is used to descramble the encrypted signal E(S) to reproduce the original signal S. A smart card containing decryption keys is therefore not required in the set-top box.

By transmitting the ECM on a separate channel from the broadcast stream, the ECM becomes individualised, i.e. it applies to an individual subscriber or group of subscribers, so that a range of new services become available. A conditional access system according to the invention enables a third party to assemble a package of channels from different service providers and distribute the package in a secure way by encrypting the package with its own control words and transmitting the control words to each subscriber via a point-to-point connection.

The above example has been described with the control word being inserted into the ECM message in unencrypted form and the ECM message being encrypted for transmission over the secure channel. In an alternative embodiment, a further level of encryption is applied by encrypting the control word CW into the ECM message, to increase the security of the conditional access system, in which case a smart card is again required in the set-top box. The smart card can be a software smart card or a virtual smart card. Alternatively, a second ECM smart card is provided as a travel smart card, so that if the first smart card for the set-top box is not in use, the second ECM smart card is used to allow point-to-point transmission of ECM messages, for example, in a roaming scenario as described below.

A conditional access system can be provided in which the possibility of roaming exists in an analogous way to roaming in a GSM network. A subscriber wishing to view a program using a set-top box arrangement in a different region from his home region requests authorisation from that region's service provider, using a travel
5 smart card as described above. The service provider checks that a subscription arrangement exists between the subscriber and his home network and, if so, transmits the control word stream required to decrypt the required program to the subscriber over a point-to-point connection.

10 Once a subscriber has requested point-to-point transmission of ECMs to his current location, the EMM information can be removed from the home region-based service by a subscriber authorisation system used by the service provider. This temporarily denies access to services at the subscriber's home location.

15 The subscriber's home region-based decoder can be a conventional decoder receiving ECMs transmitted with the broadcast stream. The decoder used at the roaming location is a decoder according to the invention, equipped to receive an ECM stream point-to-point. Two sets of ECMs are therefore being transmitted, the first multiplexed with the broadcast stream enabling viewing by the conventional
20 decoder and the second ECM stream being transmitted over a separate channel from the broadcast stream to enable a decoder according to the invention to view the programme.

To reduce the required number and calculation of ECM messages for individual
25 subscribers, the personalised ECM messages can be sent to groups of subscribers, the size of the group depending on the level of security required. A further way of reducing calculation needs is to send ECM messages for one channel only, rather than for every channel, since only the control words for the channel actually being watched need to be transferred.

30

The embodiments described above envisage the contents of the EMM messages being subsumed into the ECM messages. Of course, if it is desired to maintain the separation of the information, for example because EMM messages need to be sent

much less frequently than ECM messages, then EMM messages can continue to be sent, either incorporated in the broadcast stream, or via a separate channel, as explained for example in WO 98/43426, which is incorporated herein by reference.

For example, to block use of the home decoder in the event that the roaming

- 5 facility is used, EMM messages sent to the first decoder can indicate that subscription rights are not available while the roaming facility is in use. If the information that would conventionally be carried by an EMM message is not needed in a particular scenario, EMM messages need not be sent at all.

Claims

1. A conditional access system comprising a first transmitter for transmitting a scrambled broadcast stream and a second transmitter for transmitting a plurality of control messages separate from the broadcast stream, said control messages including information for descrambling the broadcast stream.
2. A conditional access system according to claim 1, wherein said control messages are alone sufficient to permit the broadcast stream to be descrambled.
3. A conditional access system according to claim 1 or 2, wherein said information for descrambling the broadcast stream is incorporated into each of said control messages without being encrypted.
4. A conditional access system according to claim 1 or 2, wherein said information for descrambling the broadcast stream is encrypted prior to being incorporated into each of said control messages.
5. A conditional access system according to any one of the preceding claims, further comprising a scrambler and a key generator for generating a stream of encryption keys, the scrambler being operable to encrypt a broadcast stream with the encryption key stream, the system further being operable to send the encryption key stream to a decoder for decoding the encrypted broadcast stream, said encrypted key stream comprising the information for descrambling the broadcast stream.
6. A conditional access system according to any one of the preceding claims, wherein the second transmitter is arranged to transmit the descrambling information to a receiver using a point-to-point protocol.
7. A conditional access system according to any one of the preceding claims, wherein the second transmitter is arranged to transmit the descrambling information over a secure connection.

8. A conditional access system according to claim 7, wherein the secure connection comprises a virtual private network (VPN).

5 9. A conditional access system according to any one of the preceding claims, wherein the control messages comprise entitlement control messages (ECM).

10. A conditional access system comprising a first receiver for receiving a scrambled broadcast stream and a second receiver for receiving a plurality of
10 control messages separate from the broadcast stream, the control messages including information for descrambling the broadcast stream.

11. A conditional access system according to claim 10, wherein the control messages are sent to the second receiver using a point-to-point protocol.

15 12. A conditional access system according to claim 10 or 11, wherein the control messages are sent to the second receiver over a secure connection.

13. A conditional access system according to claim 12, wherein the secure
20 connection comprises a virtual private network (VPN).

14. A conditional access system according to any one of claims 10 to 13, wherein the control messages comprise entitlement control messages (ECMs).

25 15. A conditional access system according to any one of claims 10 to 14, further comprising a decoder for descrambling the broadcast stream in accordance with the descrambling information.

30 16. A conditional access system according to any one of claims 10 to 15, wherein said information for descrambling the broadcast stream is incorporated into said control messages without being encrypted, whereby the decoder does not require a smart card for decryption.

17. A conditional access system according to any one of claims 10 to 16, wherein said second receiver comprises a mobile telephone.

18. A decoder for use in a conditional access system for decrypting encrypted broadcast content, comprising:

a first input module for receiving said encrypted broadcast content from a first communications channel;

a second input module for receiving a plurality of control messages from a second communications channel, said control messages containing descrambling information for decrypting said broadcast content.

19. A decoder according to claim 18, further comprising a processor module for extracting said descrambling information from said control messages.

20. A decoder according to claim 19, further comprising a descrambler for receiving said encrypted broadcast content and decrypting said content using said descrambling information.

21. A decoder according to any one of claims 18 to 20, wherein said descrambling information is encrypted into said control messages, the decoder further comprising a smart card for decrypting said control messages.

22. A method for use in a conditional access system, in which a scrambled broadcast stream is transmitted to a decoder, said decoder being operable to receive a plurality of control messages including information for descrambling the broadcast stream, the method comprising sending said control messages to said decoder separately from said broadcast stream.

23. A method according to claim 22, comprising incorporating said descrambling information into the control messages without encrypting it.

24. A method according to claim 23, comprising encrypting the control messages prior to sending them to the decoder.

25. A method according to claim 22, comprising sending the control messages over a secure channel.

5 26. A method according to claim 25, wherein the secure channel comprises a virtual private network.

27. A method for use in a conditional access system, in which a scrambled broadcast stream is transmitted to a first decoder and a second decoder, said first
10 and second decoders being operable to receive a plurality of control messages including information for descrambling the broadcast stream, the method comprising receiving a request to transmit a plurality of control messages to said second decoder separately from the broadcast stream.

15 28. A method according to claim 27, wherein said control messages are alone sufficient to descramble said broadcast stream.

29. A method according to claim 27 or 28, further comprising denying a service to the first decoder while the plurality of control messages is being sent to the
20 second decoder.

30. A conditional access system, comprising:

a first communications channel for carrying a broadcast stream, said stream being scrambled with a stream of control words;

25 a second communications channel separate from the first channel for carrying a stream of entitlement control messages, said entitlement control messages incorporating information relating to the stream of control words for descrambling the broadcast stream.

30 31. A conditional access system according to claim 30, wherein said entitlement control messages alone contain all of the information required to descramble the broadcast stream.

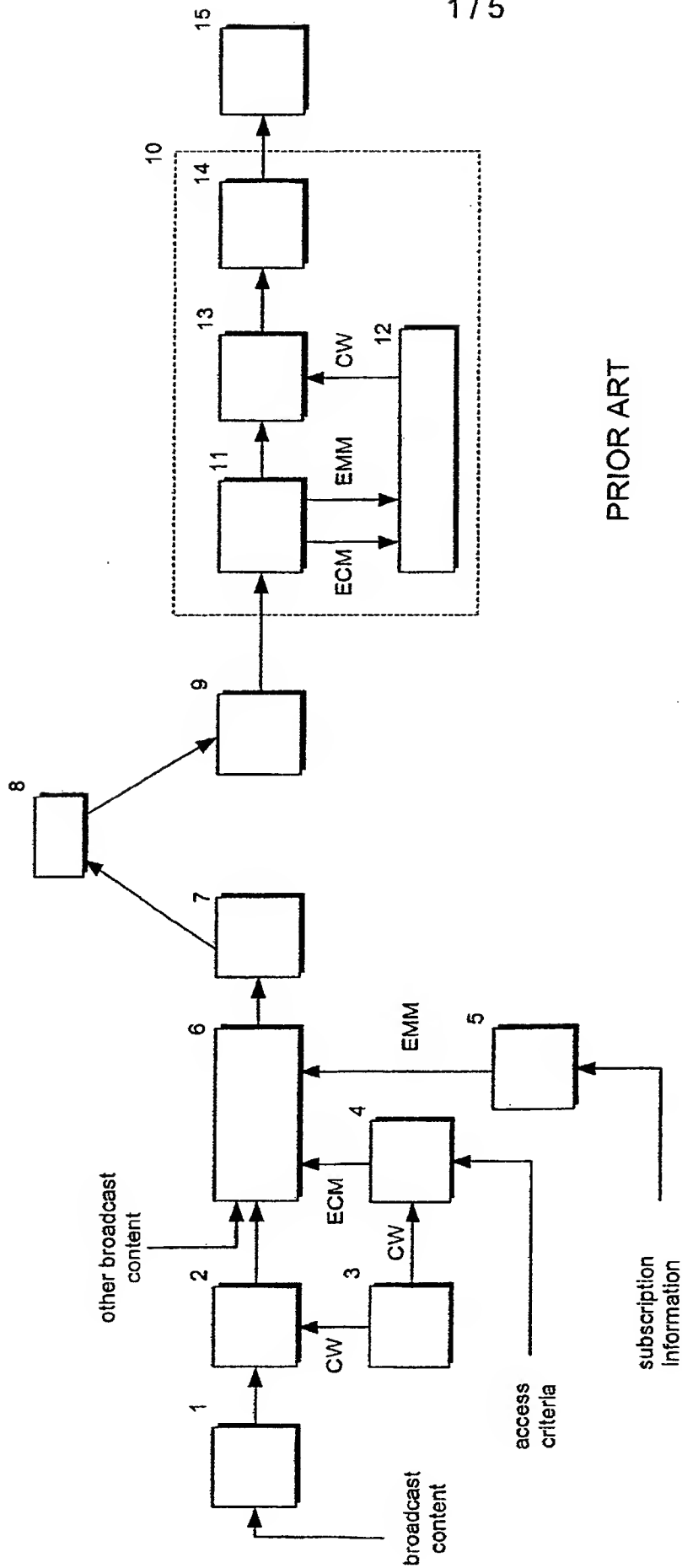


Figure 1

PRIOR ART

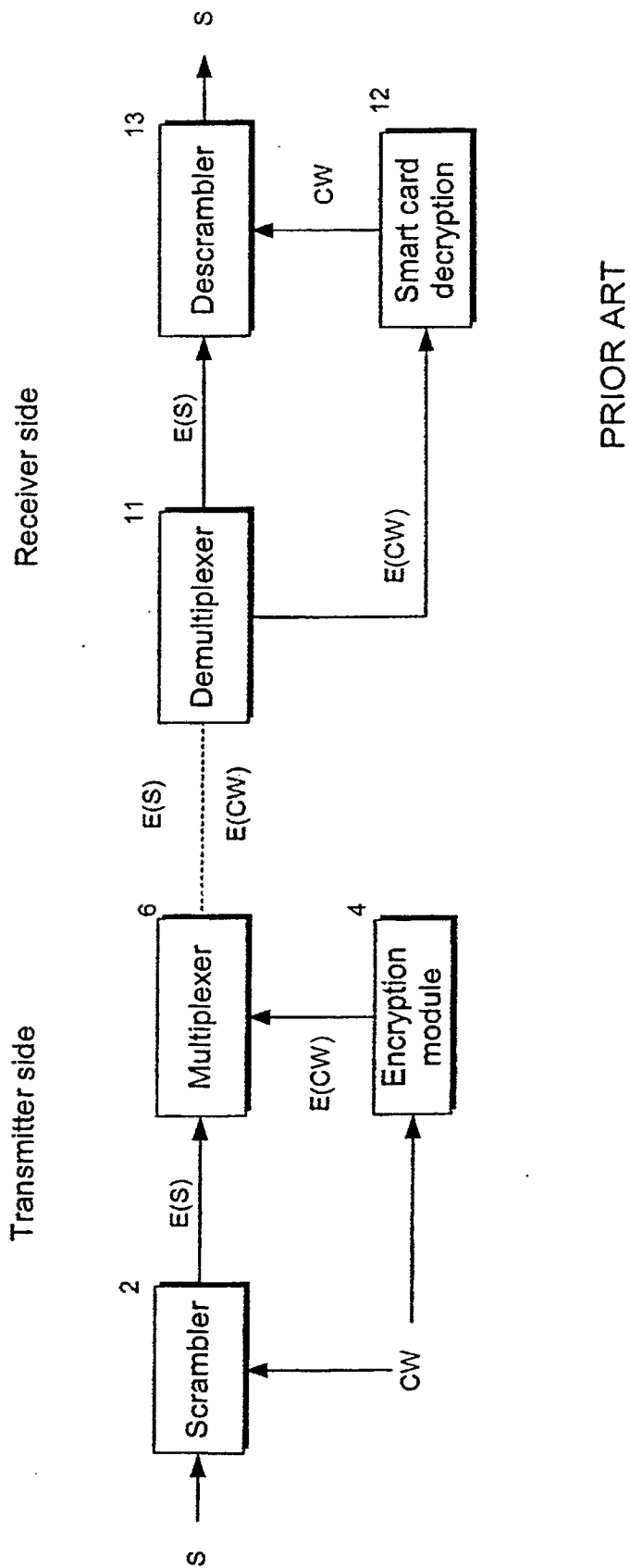


Figure 2

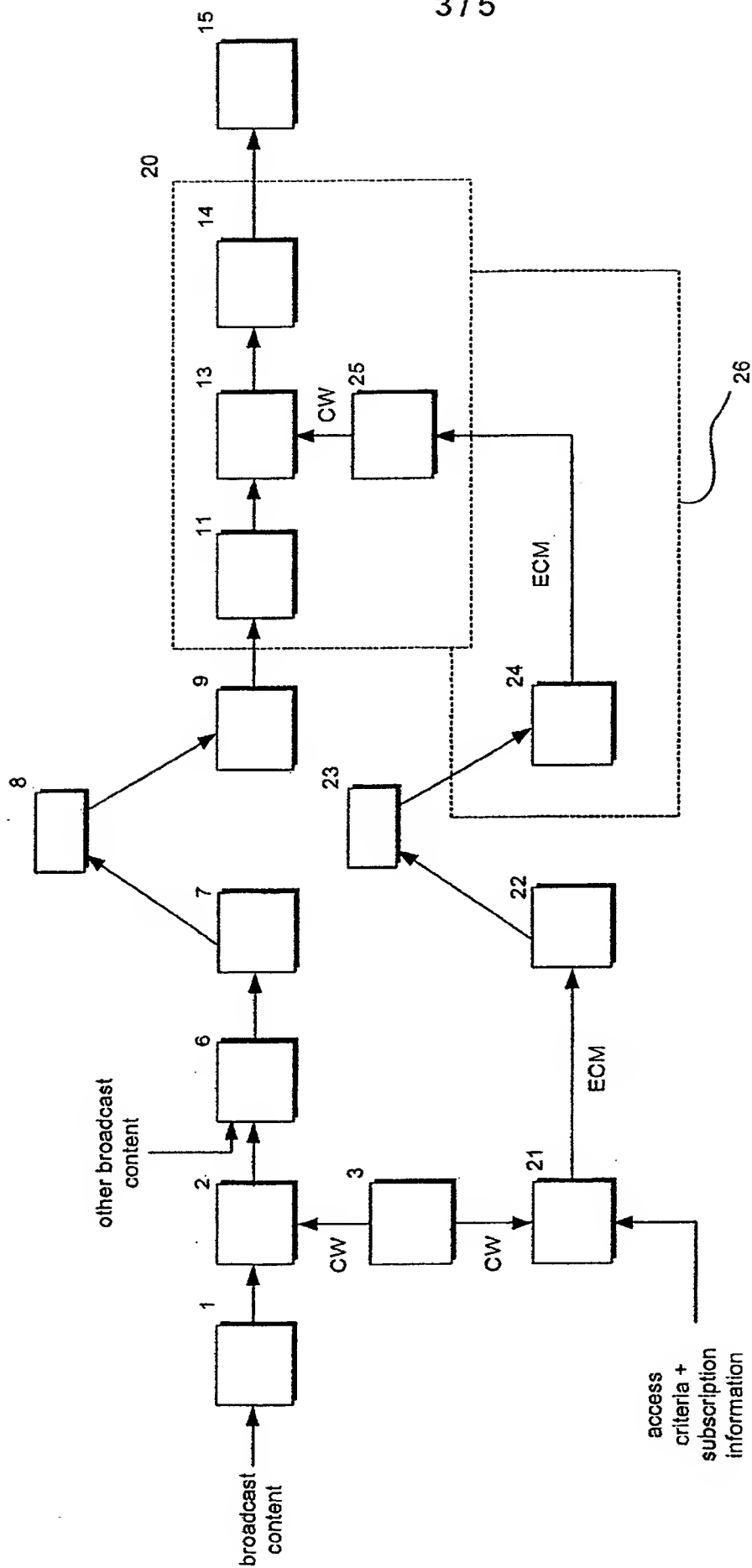


Figure 3

4 / 5

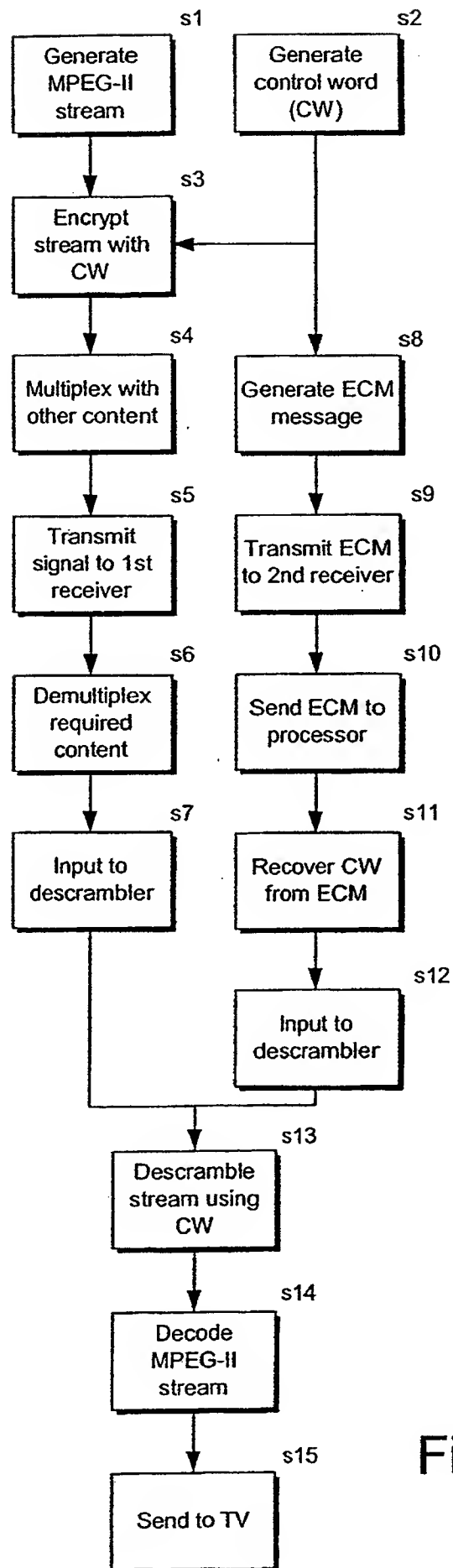


Figure 4

5 / 5

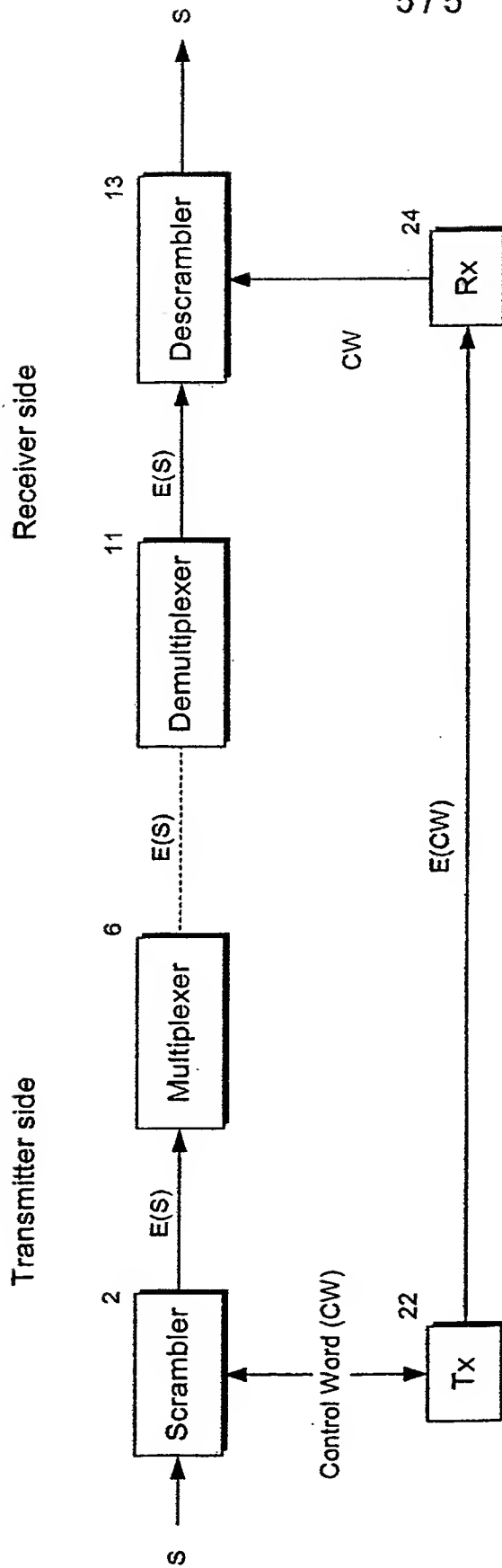


Figure 5